In the Specification:

Please amend the specification as follows:

[0001] This application is related to ~~copending~~ co-pending patent application serial No. 10/615,263 filed on July 8, 2003 and the same date ~~herewith~~ as this present application and this co-pending application claims the benefit of European patent application serial no. 03291079.6 filed May 2, 2003 entitled "Method and System for Access to Development Environment of Another " and which is also assigned to Texas Instruments Incorporated.

[0003] The complexity of system designs is increasing exponentially. This is particularly a concern for integrated circuit manufacturers such as Texas Instruments ~~Inc.~~ Incorporated. The time to market is more and more critical for success. It is believed that collaboration with customers and suppliers is the key to faster, easier, cheaper and more accurate interactions.

[0005] It is therefore an object of the present invention for manufacturer's such as Texas Instruments ~~Inc.~~ Incorporated to give access to partners such as sub-contractors, customers and Electronic Design Automation (EDA) vendors to the manufacturer's design systems computing environment without compromising Intellectual Property.

[0006] In accordance with one embodiment of the present invention access from partner's sub-contractors, customers and Electronic Design Automation (EDA) vendors to a manufacturer's (owner's) such as Texas instruments ~~Inc.~~ Incorporated design systems computing environment without compromising Intellectual Property is provided by a full suite of web-based services from design to production is provided by a highly secure network including a VPN tunnel between workstations to establish a secure encrypted tunnel end to end wherein each partner is identified with a different VPN group/password.

[0008] While executing outsourcing projects in design zones described above and in co-pending application serial no. ~~TI-35374 EP~~ 10/615,263 filed on July 8, 2003 and in European patent application serial no. 03291079.6 filed May 2, 2003 entitled "Method and System for Access to Development Environment of Another ", it is required to provide access to EDA licenses managed by FLEXLM manager running on license servers inside design zone owner's Intranet. These applications are incorporated herein by reference. This requires opening all TCP inbound connections inside the Intranet for ports greater than 1023 from all the hosts in contractor zone on which EDA applications are run. This is considered very insecure. In accordance with another embodiment of the present invention a license proxy software is provided that will act as a relay agent and route all the connections from contractor zone into the Intranet.

[0017] According to one embodiment of the present invention access from sub-contractors, customers and Electronic Design Automation (EDA) vendors to the manufacturer's such as Texas Instruments Incorporated computing environment without compromising Intellectual Property is provided by a full suite of web-based services from design to production. This interactive design compute environment in which customers can work jointly with the technical people and other representatives of Texas Instruments ~~Inc.~~ to create and test designs in a highly secure "Design Zones" promote collaboration between Texas Instruments ~~Inc.~~ (the manufacturer and owner of the computing environment) and its customers and offer flexibility in the compute and design process. Because the zones are so secure, they help ~~give~~ giving customers the confidence ~~they~~ the customers need to share design intellectual property with Texas Instruments ~~Inc.~~ Incorporated representatives and subcontractors for the purpose of completing a project and increasing the value of a joint design.

[0018] Design zones allow designers with access to the zones to compute as they would from a common UNIX desktop. They ~~login~~ log in to a highly secure Texas Instruments ~~Inc.~~ Incorporated network through the Internet, direct leased lines and/or the Texas Instruments ~~Inc.~~ Incorporated Intranet. They must pass through multiple layers of security. Once they reach the "engagement zones" Texas Instruments engineers and other representatives and their business partners can work simultaneously in multiple teams, run simulation tests, emulate software problems and share intellectual property in a secure zone.

[0019] Figure 1 illustrates Customers, Sub-contractors, and EDA Vendors (partners) accessing the Internet and through the VPN and TI external firewall 11 to the authentication 13. The access after authentication the communication then passes on to the appropriate isolated engagement boxes 15 and to the computer farm versioning storage 17. All machines in the system cannot access Texas Instruments ~~Inc.~~ Incorporated Intranet. They are blocked by the TI internal firewall 19 with the exception of the Network Time Protocol, license machines for EDA applications and a few Mail functionalities (SMPT port 25). Data produced in the system is replicated internally through the backend network or through the outside perimeter on a regular basis, and this is always initiated from inside, namely from the Intranet.

[0020] A Texas Instruments ~~Inc.~~ Design Zone security administrator monitors the activities to make sure no information leaves the site. Design engineers are restricted from removing any intellectual property from the engagement zone and a security administrator controls all movements of data. For added protection, a "co-session" management tool allows the designated zone lead engineer to monitor what the parties are doing in the zone.

[0023] Depending on the person identified by the LDAP in Step 3 above, the session will be routed to one of many engagement boxes that are on the Ethernet segments separated by Firewall boxes where in Step 4 another login/password is required and is validated thru LDAP. LDAP boxes are on the common resource segments. All users of the same partner are all launching on the same engagement box, which guarantee a high level of security. From that engagement box they have access to data and applications on the Network File System (NFS) storage system (Step 7) and access is also controlled by the LDAP mechanism for security purposes. NFS is a distributed file system from SunSoft that allows data to be shared across a network regardless of machine, operating system, network architecture or protocol. This de facto UNIX standard lets remote files appear as if they were local on a user's machine. The partners can run local applications on the engagement box (Step 5) such as design applications, mail, editor, etc or on the server farm (Step 6) that resides on the common resources segment for bigger batch or interactive jobs. Doing that, data input and output remains on the common resource, just the remote display is going back to the engagement box (X11 protocol) and therefore to the partner outside the owner (ICA) such as Texas Instruments ~~Inc.~~ Incorporated. All critical data remains in the Texas instruments ~~Inc.~~ Incorporated premises design zone. All machines in the design zone cannot access the TI Intranet because they are blocked by the firewall 19 with the exception of the Network

Time Protocol, license machines for EDA applications and a few mail functionalities (SMTP port 25). Data produced in the system is replicated internally through the backend network or through the outside perimeter on a regular basis, and this is always initiated from inside, namely from the TI Intranet via the TI internal firewall. As discussed previously a Design Zone security administrator monitors the activities to make sure no information leaves the site and design engineers are restricted from removing any intellectual property from the engagement zone and the security administrator controls all movements of data. For added protection, a "co-session" management tool allows the designated zone lead engineer to monitor what the parties are doing in the zone.

[0025] Figures 4A and 4B is a schematic diagram of the system and illustrates which protocol is allowed from where to where to guarantee security. The partners may access through the outside/business perimeter using the Internet as illustrated at the top of the drawing. A licensee may access the system trough an Intranet link. The access is through routers and thru secure mechanism such as SSH. SSH utilizes strong encryption and authentication. SSH can be installed on a private network's firewall, and a tunnel can be established from SSH client with dialup Internet access to the firewall. The input from the Internet is through VPN concentrator using a VPN tunnel. The Partners start an ICA session in a WEB page. This session is launched on a Portal machine that will authenticate through Lightweight Directory Access Protocol (LDAP) ~~the user/password~~ a user identification and password of the ~~person-~~ user. Depending on the ~~person~~ user that will authenticate through Lightweight Directory Access Protocol (LDAP) by the user identification and password ~~user/password~~ of the ~~person-~~user, then another login/password is required and is validated thru another LDAP. All users of the same partner are all launching on the same engagement box, which guarantee a high level of security. This is the second LDAP and third level of security. From that box they have access to data and applications on the Network File System (NFS) storage thru a LDAP mechanism for security purposes. There are illustrated engagement boxes 1 thru 21. The common resource segment includes the server farm, the storage NFS, DNS mail, the LDAP master and secondary LDAP. The backend Network segment includes the TI or owner's Intranet. This backend segment is mostly used for backup purposes of data in common resources as well as for data replication between Intranet and Common resource area. The async access box is used for management of all the critical boxes in the Design Zone from the Intranet thru a Terminal server box to guarantee security.

[0031] This license proxy server is run on a hardened server and the only TCP connections that need to be enabled to reach the Intranet are those from this host where the proxy is running. The proxy server can support accounting of software licenses and restrictions can be imposed for selected EDA tools based on the secure host.

[0036] The WEB proxy server is placed in the design zone and it relays the requests on behalf of the application hosts. On the firewall the ports are opened up only for the web proxy server to access the intranet web servers. This tightens the ~~seeecurity~~ security of the design zone.

[0037] Texas Instrument ~~Inc.~~ provides a full suite of web-based services to customers who do not have the system capability to connect directly to Texas Instruments ~~Inc.~~ networks. Figure ~~5~~ 7 illustrates the collaborative web-based services from design to production. At the discovery stage there are presented application solutions. At the evaluation stage there is product information, parametric search, demos, free evaluation tools, free samples and tools eStore. At the design/test stage there is training/Webcasts, third party network, update advisor, technical support, knowledge base and discussion groups. At the production stage there is availability information and lead time information.

[0038] Figure ~~6~~ 8 illustrates the collaborative process from design through shipping and receiving. In the design stage the collaborative design services include secure collaborative design zones, linked IT infrastructures across design partners, web-based program management and product delivery workflow tools and customer co-simulations and consolidated design storage. During planning and forecasting the services are short and long term forecasting and response, proactive messaging/alerts, replenishment models adapted to customer needs, and leading on RosettaNet standards related to planning and forecasting. During order management the services are quote management (create and change), order management (create and change and status), order acknowledgements, material tracking (ship notices, inventory, WIP), and leading on EDI, RosettaNet, and barcode standards usage and definition. The collaborative services for supplier for manufacturing include electronic-catalog for self-service ordering, multiple integration options (EDI/RosettaNet, XML or Web), Web contract management, material specification available via the Web, Web PO, invoice and acknowledgement, and logistics track and trace. The collaborative services for subcontractors for manufacturing include forecast management, purchase order management, inventory management, planning management, receiving management and shipment tracking. The distributor collaboration services during shipping and receiving include multiple integration options (EDI, RosettaNet, Web), quote management (create and change), order management (create, change, and status), order acknowledgements, shipment notices and tracking, price list, ship and debit processing, design registration, inventory reporting and resale management.